Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/GB05/001709

International filing date: 04 May 2005 (04.05.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/572,434
Filing date: 19 May 2004 (19.05.2004)

Date of receipt at the International Bureau: 31 May 2005 (31.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PA 1301710

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

April 01, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE UNDER 35 USC 111.

APPLICATION NUMBER: ***60/572,434***
FILING DATE: ***May 19, 2004***

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

P. SWAIN
Certifying Officer

11324 U.S.PTO

Please type a plus sign (+) inside this box → [+]

PTO/SB/16 (5-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

13441 U.S.PTO 60/572434

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
John Fleming	WALKER	United Kingdom

☐ *Additional inventors are being named on the ____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (280 characters max)

CHIP SHIELDING SYSTEM AND METHOD

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number [ ] → *Place Customer Number Bar Code Label here*

OR *Type Customer Number here*

☒ Firm *or* Individual Name	L. Friedman, Welsh & Katz, Ltd.				
Address	120 S. Riverside Plaza, 22nd Floor				
Address					
City	Chicago	State	Illinois	ZIP	60606
Country	USA	Telephone	312-655-1500	Fax	312-655-1501

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages*	8	☐ CD(s), Number	
☒ Drawing(s) *Number of Sheets*	2	☐ Other (specify)	
☐ Application Data Sheet. See 37 CFR 1.76			

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT *(check one)*

FILING FEE AMOUNT ($)

☒ A check or money order is enclosed to cover the filing fees

☒ The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number 23-0920

☐ Payment by credit card. Form PTO-2038 is attached.

$160.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE

Date 5/19/04

REGISTRATION NO. *(if appropriate)* 37,135

Docket Number: 7251/92170

TYPED or PRINTED NAME L. Friedman

TELEPHONE 312-655-1500

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

P19LARGE/REV05

PTO/SB/17 (10-03)
Approved for use through 07/31/2006. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL for FY 2004

Effective 10/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) **$160.00**

Complete if Known	
Application Number	
Filing Date	19 May 2004
First Named Inventor	John Fleming WALKER
Examiner Name	
Art Unit	
Attorney Docket No.	7251/92170

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money ☐ Other ☐ None

☐ Deposit Account:

Deposit Account Number: 23-0920

Deposit Account Name: Welsh & Katz, Ltd.

The Director is authorized to: *(check all that apply)*

☐ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s) or any underpayment of fee(s)

☐ Charge fee(s) indicated below, except for the filing fee to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	770	2001	385	Utility filing fee	
1002	340	2002	170	Design filing fee	
1003	530	2003	265	Plant filing fee	
1004	770	2004	385	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	160.00

SUBTOTAL (1) ($) **$160.00**

2. EXTRA CLAIM FEES FOR UTILITY AND

	Extra Claims		Fee from below	Fee Paid
Total Claims	-20** =	0	X =	0.00
Independent Claims	- 3** =	0	X =	0.00
Multiple Dependent			=	

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	86	2201	43	Independent claims in excess of 3
1203	290	2203	145	Multiple dependent claim, if not paid
1204	86	2204	43	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) **$0.00**

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non - English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	420	2252	210	Extension for reply within second month	
1253	950	2253	475	Extension for reply within third month	
1254	1,480	2254	740	Extension for reply within fourth month	
1255	2,010	2255	1,005	Extension for reply within fifth month	
1401	330	2401	165	Notice of Appeal	
1402	330	2402	165	Filing a brief in support of an appeal	
1403	290	2403	145	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,330	2453	665	Petition to revive - unintentional	
1501	1,330	2501	665	Utility issue fee (or reissue)	
1502	480	2502	240	Design issue fee	
1503	640	2503	320	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR § 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Statement	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	770	2809	385	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	770	2810	385	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	770	2801	385	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) ($)

SUBMITTED BY

Name (Print/Type)	L. Friedman	Registration No. (Attorney/Agent)	37,135	Telephone	312-655-1500
Signature				Date	19 May 2004

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Patentee:	WALKER, John Fleming
Title:	CHIP SHIELDING SYSTEM AND METHOD
Serial No.:	
Filing Date:	19 May 2004
Docket No.	7251/92170

Certificate of Express Mailing

Express Mail mailing label number EL 996734637 US

Date of Deposit: 19 May 2004

I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail" Post Office to: Mail Stop Provisional Patent Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450. This mailing includes Provisional Application Cover Sheet (1 pg); Fee Transmittal (1 pg) in duplicate; Check in the amount of $160.00; Specification (8 pgs) and Drawings (2 sheets); Application Data Sheet (2 pgs); and return receipt postcard.

The person mailing this paper is:

John Austin Rembert
Typed or Printed Name of Person Mailing Paper of Fee

John Rembert
Signature of Person Mailing Paper or Fee

Application Data Sheet

Inventor Information

Inventor One Given Name::	John Fleming
Family Name::	WALKER
Postal Address Line One::	1 Malyns Close
City::	Chinnor, Oxon
Country::	United Kingdom
Postal or Zip Code::	OX39 4EW
Citizenship Country::	United Kingdom

Correspondence Information

Name Line One::	Welsh & Katz, Ltd.
Name Line Two::	L. Friedman
Address Line One::	22nd Floor
Address Line Two::	120 South Riverside Plaza
City::	Chicago
State or Province::	IL
Postal or Zip Code::	60606
Telephone Number::	(312) 655-1500
Fax::	(312) 655-1501

Application Information

Title Line One::	CHIP SHIELDING SYSTEM AND METHOD
Total Drawing Sheets::	2
Application Type::	Provisional
Docket Number::	7251/92170

Representative Information

Registration Number One::	24,003
Registration Number Two::	22,839
Registration Number Three::	28,903
Registration Number Four::	27,429
Registration Number Five::	25,060
Registration Number Six::	22,053
Registration Number Seven::	27,466
Registration Number Eight::	29,434
Registration Number Nine::	29,054
Registration Number Ten::	29,381
Registration Number Eleven::	34,044
Registration Number Twelve::	27,600
Registration Number Thirteen::	34,137
Registration Number Fourteen:	38,110
Registration Number Fifteen::	39,724
Registration Number Sixteen:	39,021
Registration Number Seventeen:	37,963
Registration Number Eighteen:	37,135
Registration Number Nineteen:	40,604
Registration Number Twenty:	37,435
Registration Number Twenty-One:	45,195
Registration Number Twenty-Two:	40,687
Registration Number Twenty Three:	41,050

Assignee Information

Assignee Name: NDS Limited

Assignee Address: One London Road
Staines, Middlesex TW18 4EX
United Kingdom

CHIP SHIELDING SYSTEM AND METHOD

FIELD OF THE INVENTION

The present invention relates to protecting integrated circuit chips from invasive attack through the use of a shield.

BACKGROUND OF THE INVENTION

Security chips are of use to those wanting to protect information, data transmissions or value (typically monetary). These security chips protect data by storing it in secure memory or transmit data securely through the use of cryptography implemented on chip. There are many reasons for using these products including secure banking cards, secure access systems and secure personal identity systems. It is known in the art to protect these chips from invasive attacks whereby criminals and other agents attack the card to try to obtain, change or use secret information on the card.

One type of attack involves trying to place contacts onto internal chip nodes in order to read internal data traffic. This may be achieved by probing, using fine needles to break through the surface passivation to reach the fine metal tracks. Alternatively focused ion beam (FIB) may be used to deposit pads of metal onto the tracks for subsequent probing or bonding by wires. However it is achieved, measuring the signals on internal chip nodes represents an attack, and if successful this attack may render the chip and entire system on which it is based, insecure.

Shields to protect a chip from the above attacks exist at present; they are typically divided into two categories, active and passive. Passive shields are simple metal layers over all or part of the circuit and are designed to prevent viewing and probing. Passive shields may be removed by chemical, plasma or other techniques without changing the operation of the circuit. In other words, a passive shield works to deter attackers by making viewing more difficult initially, but will not actively defend itself against removal.

Active shields may look similar or may look more like a network of lines covering all or part of a circuit. If a line or part of the shield is removed,

severed or short-circuited to another line, the breach is detected and the chip halts some or all functions.

Active shields may still be breached using, for example, the following technique. An active shield line is identified as above the circuit element to be attacked. This shield line is bypassed using the ability of the FIB system previously mentioned. The bypass is in the form of a diversion track added in parallel to the original shield track. The original shield track may now be removed leaving the new bypass to fool the detection circuit. No circuit break is detected.

SUMMARY OF THE INVENTION

The present invention, in preferred embodiments thereof, comprises an active shield made in such a way that individual tracks are not visible by any normal microscopy technique. The tracks are preferably present in a layer of semiconductor material. The tracks preferably comprise doped regions separated by semi-insulating regions of either undoped material, or differently doped material. The tracks are doped sufficiently to allow conduction of electronic carriers. Between the tracks, the material, doped or undoped, is depleted of carriers. This region is rendered semi-insulating through the lack of intrinsic or extrinsic carriers, or through the trapping of such carriers. The conductive region is formed into tracks which form part of an active shield as described above. Most preferably, the conductive lines and the insulating regions between them are made in the same way and look identical to all analytical techniques. An attacker therefore does not know where to bypass the active shield lines.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention; and

Fig. 2 is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

The present invention, in preferred embodiments thereof, provides a method to protect a security chip from invasive attacks. Preferably, a layer is added above the layers of the circuit to be protected from attack. The added layer may be made of polycrystalline silicon, as this material is commonly used in the manufacturing cycle of integrated circuits, but may alternatively be made of many other suitable materials. Any material whose conductivity can be materially changed without being visibly different would be a candidate for the material to be used in the added layer. The added layer is typically applied towards the end of the chip manufacturing process, and is applied above the normal circuit interconnect layers. The added layer may also be protected by a passivation layer, as is typically used in such integrated circuits.

The added layer is preferably implanted with dopants to allow conduction. In one preferred embodiment of the present invention dopants are selectively implanted in tracks corresponding to where the designer wants them placed. Dopants may be implanted in the material by high energy ion bombardment or by any other appropriate method.

In another preferred embodiment of the present invention utilizes either blanket bombardment of the layer with dopant ions or incorporation of the dopants during the growth of the layer. This latter approach will typically be achieved in the case of doped polysilicon, by CVD growth using silane gas for silicon growth and boron trichloride gas for dopant species.

However the growth and dopant incorporation is achieved, it must be done in such a way that the incorporated dopant atoms are not active. This means that the dopant atoms are not on designated sites as substitutes for the main material atoms. This means that the dopant atoms are interstitial, or between their normal, substitutional sites. This further means that the dopant atoms do not contribute carriers to conduction processes in the layer. This means that the material, as grown, is semi-insulating and does not conduct.

A further step in the creation of the shield layer is the selective activation of the dopants described above. The selective activation is typically achieved through an annealing process. This annealing process is effective if the

material is heated to a temperature close to (typically, within approximately 100 degrees C of) its melting point. In one preferred embodiment, the doped polysilicon is rapidly brought up to the annealing temperature by irradiation from a pulsed light source. The pulsed light source may be an infrared laser. The laser may be a YAG laser (Yttrium Aluminium Garnet, output wavelength 1064 nm). This laser may be driven in pulsed mode with a q-switch to limit the on-time to several nanoseconds or faster. The high power density during the pulse must be sufficient to anneal the dopants in that region of the material. In addition, the power density during the pulse must not be sufficient to ablate the material or cause damage to active circuit layers.

Conductive tracks are patterned into the layer by the annealing action. The laser, for example, may be scanned across the surface. The pattern of scanning is immaterial but may be raster scanning or following the semi-random path of a tracks path from start to end, or most efficiently, by alternate direction scanning (boustrephorous scanning) of the surface. The annealing will locally activate the dopants in the tracks required.

The annealing must be such that the conductive tracks are physically similar in all important respects to the semi-insulating material between the tracks. An attacker cannot "see", by normal analytical means, the tracks to be bypassed in an attack.

Reference is now made to Fig. 1, which is a simplified pictorial illustration of an integrated circuit protected by chip shielding, constructed and operative in accordance with a preferred embodiment of the present invention. This figure shows the basic construction of an integrated circuit with a silicon (single crystal) substrate on top of which are constructed gates and other active and passive circuit elements interconnected by networks of (typically) aluminium tracks. As these aluminium tracks are vulnerable to attack a layer of polysilicon is shown above them to illustrate the position of the protective shield layer.

Reference is now made to Fig. 2, which is a simplified pictorial illustration of a top view of the integrated circuit of Fig. 1. This figure shows a top down view of the protective shield layer. The serpentine track illustrates one method, as described above, of writing a serpentine conductive line in this

material. As described above, this can be achieved by scanning a pulsed infra-red laser over the areas to be annealed. The annealing activates the dopants in this region, allowing conduction along the track. The track may be connected to the underlying circuitry using, for example, tungsten plugs as vias.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow:

What is claimed is:

CLAIMS

1. Apparatus substantially as described hereinabove.

2. Apparatus substantially as shown in the drawings.

3. A method substantially as described hereinabove.

4. A method substantially as shown in the drawings.

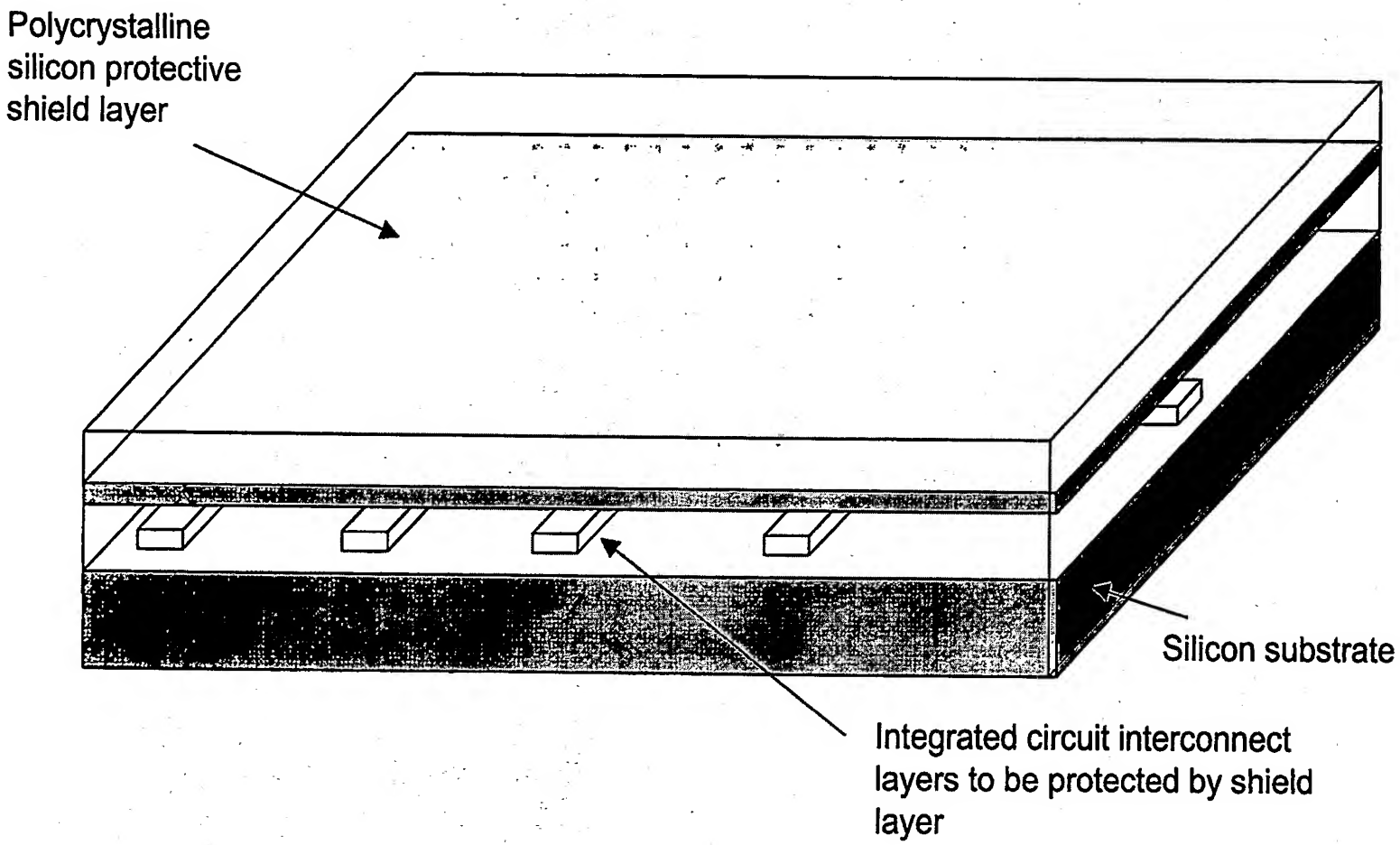

Fig. 1

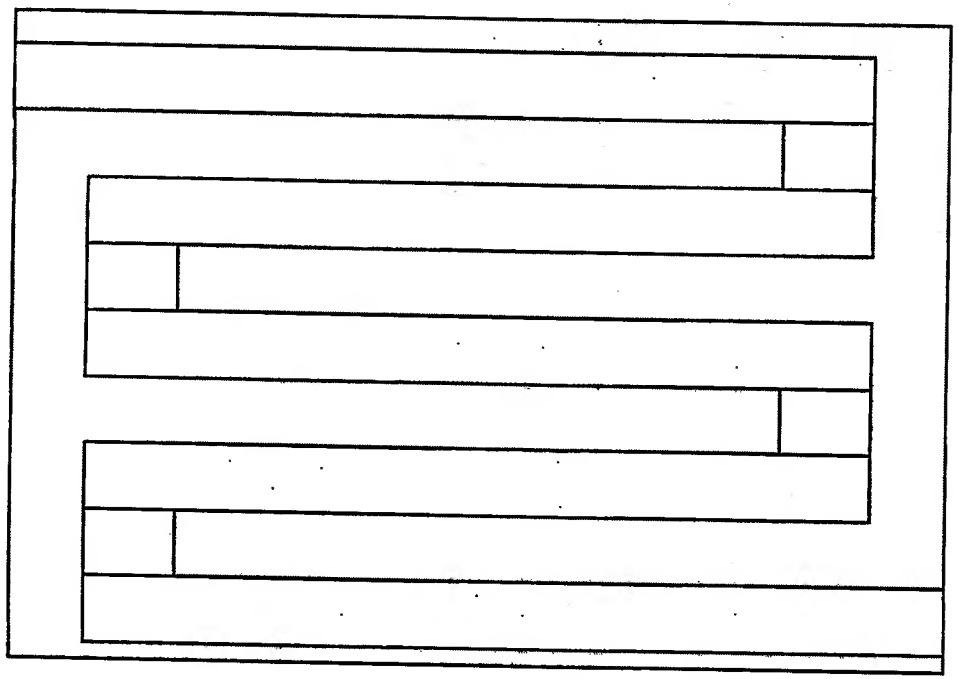

Fig. 2